UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/644,515	08/20/2003	Jonathan D. Beard	TUC920030115US1 (16874)	6578

46263 7590 11/13/2008
SCULLY, SCOTT, MURPHY, & PRESSER, P.C.
400 GARDEN CITY PLAZA
SUITE 300
GARDEN CITY, NY 11530

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
11/13/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/644,515	BEARD ET AL.	
	Examiner	Art Unit	
	Thomas Gyorfi	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 September 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 remain for examination. The correspondence filed 9/2/08 amended claims 1, 10-12, 20, 21, and 28-30.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 9/2/08 has been entered.

Response to Arguments

3. Applicant's arguments filed 9/2/08 have been fully considered but they are not persuasive. Applicant primarily argues:

> On the other hand, independent claims as amended in the present application recite, "the encrypted login information and authentication information associated with the user being in an encrypted format that cannot be accessed by the user machine when the user machine communicates the encrypted login information and authentication information to the authentication server.., no direct connection being needed between the client machine and the authentication server to authenticate the user's access to the client machine" Unlike the claims in the present application, both Guo et al. and Soto et al. require that the user enter a specific username and password accessible or known to the user and that client machine and the machine that performs authentication (i.e., authentication server in Guo et al. and remote access server in Soto et al.) communicate for authenticating the user. For example, while the Examiner cited paragraph [0051] of Guo et al. refers to an encrypted ticket, that ticket is communicated directly from the authentication server to the client machine (affiliate server). Without such login and communication schemes between their client machines and authentication servers, Guo et al. and Soto et al.'s authentication mechanism would not work.

Examiner fails to see how this argument would establish an alleged difference between the claims (particularly with the new limitation) and the prior art. As Applicant noted, the ticket that is passed between the authentication server and the affiliate server is encrypted with a session key that is intended to be known only by those two servers and not the user's machine (paragraphs 0038 and 0048). As a result, the encrypted ticket, which is passed between said servers by way of the user machine via the well known technique of HTTP redirection (thus satisfying the "no direct connection" limitation: see paragraphs 0048-0049), cannot be decrypted by the user machine because it does not, and cannot, have the session key with which the ticket is encrypted. Additionally, it is observed that just because the user may likely already know what one's username and password for a particular affiliate server are, this has no bearing on the claims because the claims do not actually recite a limitation to the login information has to be created during the course of the authentication procedure. While it is observed that the claims include limitations of "creating an encrypted login information", this is strictly speaking different from "creating login information, encrypting said login information," and then subsequently using said encrypted login information in the claimed authentication process; as the former case does not preclude the use of usernames and passwords that were already known by the user to be supplied for encryption.

With respect to Applicant's remaining arguments, upon further consideration it is observed that Guo appears to disclose an alternate embodiment wherein the login information is not encrypted as it sent to the user machine: see paragraphs 0053-0055.

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guo (U.S. Patent Application Publication 2003/0217288) in view of Soto et al. (U.S. Patent Application Publication 2003/0208695).

Regarding claims 1, 10-12, 20, and 21:

Guo discloses a method/system/program for authenticating a user's access to a client machine, comprising: communicating a request for access from the user machine to the client machine (paragraph 0045; element 32 of Figure 3); establishing a login account with login information in response to the request (paragraph 0032); encrypting the login information at the client machine and communicating the encrypted login information to the user machine (paragraph 0047); communicating the encrypted login information and authentication information associated with the user from the user machine to an authentication server (Ibid, and element 50 of Figure 3), the encrypted login information and authentication information associated with the user being in an encrypted format that cannot be accessed by the user machine when the user machine communicated the encrypted login information and authentication information (the ticket being encrypted by a session key that only the servers and not the user machine have access to: paragraphs 0038, 0048, and 0049); and decrypting the encrypted login information at the authentication server and communicating the decrypted login

information to the user machine if the authentication information is acceptable to the authentication server (paragraphs 0039-0040, and 0049- 0050), no direct connection being needed between the client machine and the authentication server to authenticate the user's access to the client machine (communication between servers is done by the user machine via HTTP redirects: paragraphs 0046-0049). For the sake of clarity, it is noted that the "client machine" of Guo corresponds to the user machine of the claim, and the affiliate server(s) of Guo correspond to the "client machine" of the claim.

Guo does not explicitly disclose wherein it is the client machine that establishes the user account and communicates the information to the user machine. However, Soto discloses this limitation (paragraphs 0046-0055, but particularly 0053-0055). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Guo to allow for a client machine to create temporary accounts for a user (such as used by a technician or engineer) and securely communicate such information to the user machine, as disclosed by Soto. The motivation for doing so would be to expedite the process of allowing users to login to a machine for service and maintenance without waiting for days for a new account and without compromising security (Soto, paragraph 0004).

It is noted that the login information (including but not limited to usernames and passwords) is known and would be encrypted at its source(s) and subsequently decrypted at its destination(s), as those of ordinary skill in the art would have long since known that sending said login information over a network in an unencrypted fashion was a serious security risk which could otherwise defeat the security afforded by the prior art

inventions (see the previously cited "Eliminating Plaintext Passwords on Your Network" reference). Also note that Guo discloses using SSL – a known solution to the aforementioned problem clearly within the technical grasp of one of ordinary skill in the art – in that invention (paragraph 0039). Accordingly, if using SSL to encrypt and decrypt the login information would lead to the anticipated success, it is likely the product not of innovation but of ordinary skill and common sense. *KSR v. Teleflex*, 550 U.S. at ___, 82 USPQ2d at 1397.

Regarding claims 2, 13, and 22:

Guo and Soto disclose all the limitations of claims 1, 12, and 21 above. Guo further discloses communicating an identifier associated with the user from the user machine to the client machine (paragraph 0038); encrypting the identifier at the client machine and communicating the encrypted identifier to the user machine (paragraph 0047); communicating the encrypted identifier from the user machine to the authentication server (Ibid, and element 50 of Figure 3); decrypting the encrypted identifier at the authentication server (paragraphs 0039-0040); wherein the decrypted login information is communicated to the user machine if the decrypted identifier is acceptable to the authentication server (Ibid, and paragraphs 0049-0050).

Regarding claims 3, 14, and 23:

Guo and Soto disclose all the limitations of claims 1, 12, and 21 above. Guo further discloses encrypting the identifier at the client machine and communicating the

encrypted identifier to the user machine (paragraph 0047); communicating the encrypted identifier from the user machine to the authentication server (Ibid, and element 50 of Figure 3); decrypting the encrypted identifier at the authentication server (paragraphs 0039-0040); wherein the decrypted login information is communicated to the user machine if the decrypted identifier is acceptable to the authentication server (paragraphs 0049-0050).

Regarding claims 4, 15, 24, and 28-30:

Guo and Soto disclose all the limitations of claims 1, 12, and 21 above. Guo further discloses communicating the login information from the user machine to the client machine to enable the user to access the client machine (paragraph 0049; element 60 of Figure 3). As claims 28-30 consist of all the limitations of claim 4, they are rejected by the same rationale.

Regarding claims 5, 16, and 25:

Guo and Soto disclose all the limitations of claims 1, 12, and 21 above. Guo further discloses wherein the login information comprises at least one of a name and a password (paragraph 0032).

Regarding claims 6, 17, and 26:

Guo and Soto disclose all the limitations of claims 1, 12, and 21 above. Guo further discloses wherein the login information is encrypted at the client machine using a

public key of a public key-private key pair (paragraph 0040); and the encrypted login information is decrypted at the authentication server using the private key of the public key-private key pair (Ibid).

Regarding claims 7, 18, and 27:

Guo and Soto disclose all the limitations of claims 1, 12, and 21 above. Guo further discloses wherein the authentication identifier comprises an identifier associated with the user (paragraph 0032).

Regarding claims 8 and 19:

Guo and Soto disclose all the limitations of claims 1 and 12 above. Guo further discloses wherein the encrypted login information is inaccessible to the user machine (paragraph 0051).

Regarding claim 9:

Guo and Soto disclose all the limitations of claim 1 above. Guo further discloses wherein the request for access is communicated from the user machine to the client machine, and the encrypted login information is communicated from the client machine to the user machine via a Secure Sockets Layer connection (paragraphs 0039 & 0055).

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- Wikipedia article on "Transport Layer Security" from 8/4/03
- "SSL 3.0 Specification" (from the Internet Archive on 3/1/01)

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
11/6/08
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435